UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF GEORGIA ATLANTA DIVISION

SABINA BOLOGNA, an individual; LUCIA LAROCCHIA, an individual; EMILY KNOWLES, an individual; and KRISTEN GALLOWAY, an individual, on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

EQUIFAX, INC.,

Defendant.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

I. INTRODUCTION

1. This class action is brought against Defendant Equifax, Inc ("Equifax"), based on its failure to protect, secure, and safeguard the personally identifiable information ("PII") of the plaintiffs, including approximately 143 million other United States consumers. Equifax is a consumer credit reporting agency and failed to protect the PII it collected from various sources. Equifax also failed to timely and adequately notify the plaintiffs and the Class that their PII had been compromised due to a cybersecurity

breach, which Equifax had failed to guard against. ***Equifax has also traced the data breach to a software problem that, upon and information and belief, it discovered in March 2017. This software problem could have been remediated promptly, but Equifax failed to do so.***

II. PARTIES, JURISDICTION, AND VENUE

2. Plaintiff Sabina Bologna is a citizen and resident of Whitefish, Montana, and was harmed because of the events giving rise to the claims set forth herein.

3. Plaintiff Lucia Larocchia is a citizen and resident of North Las Vegas, Nevada, and was harmed because of the events giving rise to the claims set forth herein.

4. Plaintiff Emily Knowles is a citizen and resident of Northampton, Massachusetts, and was harmed because of the events giving rise to the claims set forth herein.

5. Plaintiff Kristen Galloway is a citizen and resident of Ellenwood, Georgia, and was harmed because of the events giving rise to the claims set forth herein.

6. Defendant Equifax, Inc is a Delaware corporation with its principal place of business located at 1550 Peachtree Street NE Atlanta, Georgia 30309.

Equifax can be served with process through its registered agent, Shawn Baldwin, at 1550 Peachtree Street NE Atlanta, Georgia 30309.

7. The Court has jurisdiction under the Class Action Fairness Act, 28 U.S.C. 1332(d)(2). The amount in controversy exclusive of interest and costs exceeds $5 million. Minimal diversity exists and there are over 100 putative class members.

8. Equifax maintains its principal place of business in Georgia and is therefore a citizen of Georgia for personal jurisdiction purposes. Venue is proper under 28 U.S.C. § 1391 because Equifax maintains its principal place of business in this District and a substantial part of the events or omissions giving rise to the claims set forth herein occurred in this District.

III. FACTUAL ALLEGATIONS

9. On or about September 7, 2017, Equifax made public a cybersecurity incident (the "data breach"), which involves approximately 143 million United States consumers. Equifax disclosed that, between mid-May and July 2017, hackers infiltrated their cyber security system and accessed consumer data, including names, social security numbers, birth dates, addresses, and driver's-license numbers. Equifax has also disclosed that both credit card information for approximately 209,000 United States consumers and documents used in disputes for 182,000 people were also

siphoned during the breach. The incident is among the largest and most severe cybersecurity breaches in history.

10. Equifax claims it discovered the breach on July 29, 2017.

11. On August 1, 2017, three Equifax senior executive sold shares of stock worth almost $1.8 million. Equifax's Chief Financial Officer (CFO) John Gamble sold company shares worth $946,374 (13% of his stake in Equifax); Joseph Loughran, Equifax's president of United States information solutions, exercised options to dispose of stock worth $584,099 (9% percent of his stake in Equifax); and, on August 2, 2017, Rodolfo Ploder, Equifax's president of workforce solutions, sold $250,458 of stock (4% of his stake in Equifax). A spokeswoman for Equifax said "[the executives] had no knowledge that an intrusion had occurred at the time [they sold the shares]".

12. Equifax has traced the data breach to a software flaw that, upon information and belief, it detected in March 2017, which flaw could have been remediated with a software patch well prior to the data breach.

13. Equifax is one of three credit bureaus in the United States that tracks the financial history of consumers to calculate and report a score that is to be used by lenders, employers, or any other person or entity interested in a person's creditworthiness. The company is supplied with a broad range of

personal and financial data, including loans, loan payments, credit cards, child support payments, credit limits, missed payments, addresses, and employer history.

14. Not everyone affected by the data breach is aware that Equifax held their PII. Equifax obtains much of its data from those who report the credit activity of consumers, including credit card companies, banks, retailers, and lenders.

15. PII is valuable to cybercriminals who operate on hidden Internet websites like darknets and overlay networks (a.k.a., the "dark web"). Identity thieves can use stolen PII as their own—to open new financial accounts, to take out loans in another's name, incur charges on existing accounts, or clone ATM, debit, or credit cards.

16. Equifax either knew or should have known it had a duty to protect and safeguard consumers' PII. Equifax also either knew or should have known of the importance of safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached, including the significant costs that would be imposed on consumers because of a breach.

17. At all relevant times, Equifax was fully aware it maintained the PII of a substantial number of persons. Equifax also knew that if this highly sensitive data was breached, then a substantial number of persons would

probably be harmed. Nonetheless, Equifax's approach to maintaining the privacy and security of Plaintiffs and the Class was reckless, wanton, and/or negligent.

18. Identity theft is a known, serious, and growing threat. Javelin Strategy & Research reported that identity thieves have stolen approximately $112 billion over the past six years. [1]

19. When a data breach occurs, there may be delays between the times when the breach occurs, when the breach is discovered, and when PII is stolen, sold, or used.

20. Now, Plaintiffs and the Class must constantly monitor their financial and personal records for an indefinite period of time. Plaintiffs and the Class are incurring and will continue to incur such damages in addition to any misuse of their PII.

21. The PII of Plaintiffs and the Class is private, highly sensitive, and was inadequately safeguarded by Equifax. Moreover, Equifax did not obtain consent to disclose the PII to any third person, as required by applicable laws and regulations.

---

[1] Pascual et al, *2016 Identity Fraud: Fraud Hits an Inflection Point*, Javelin, February 2, 2016, available at https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited September 11, 2017).

22. The data breach was a direct and proximate result of Equifax's failure to properly protect Plaintiffs' and Class members' PII from unauthorized access, use, and disclosure, as required by state and federal regulations, industry practices, and common law. Equifax failed to maintain appropriate, administrative, technical, and physical safeguards to ensure the security and confidentiality of PII and to protect against reasonably foreseeable threats to the security and integrity of PII.

23. Equifax had the resources to prevent a breach, but failed to adequately invest in data security, despite the growing number of well-publicized data breaches.

24. Had Equifax remedied the deficiencies in its data security systems, followed security guidelines, and adopted security measures as recommended by experts in the field, Equifax probably would have prevented the data breach, the resulting theft of PII, and the increased risk of identity theft.

25. As a direct and proximate result of Equifax's conduct and the resulting data breach, Plaintiffs and the Class have been placed at an increased, imminent, and continuing risk of identity theft and identity fraud. As a direct and proximate result of the risks of increased risks, affected persons must spend time to mitigate the potential impact of the data breach,

including “freezes” and “alerts” with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, closely reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports.

26. Equifax directly and proximately caused the risk of disclosure and acquisition of the PII of Plaintiffs and the Class, causing them to suffer and to continue to suffer economic damages and other actual harm for which they are entitled to compensation, including but not limited to:

a. Risk of theft for personal and financial information;

b. Unauthorized charges on debit and credit card accounts;

c. The potentially severe injury flowing from fraud and identity theft;

d. The untimely and inadequate public disclosure of the data breach;

e. The improper disclosure of PII;

f. Loss of privacy;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of time spent to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of PII;

i. Ascertainable losses in the form of lost rewards, because of the inability to use certain accounts and cards affected by the data breach;

j. Loss of use and access to account funds and costs associated with the inability to obtain money from compromised accounts or greater

limits in the amount of money able to be obtained from the accounts, including missed payments, late charges, fees, and adverse effects to credit reports, scores, and information; and

k. The loss of productivity and value of time spent to mitigate the consequences of the data breach, including the discovery of fraudulent charges, cancellation and reissuance of cards, the purchase of credit monitoring and identity-theft-protection services, imposition of withdrawal and purchase limits on compromised accounts, and the pain, suffering, and mental anguish secondary to the data breach and resulting consequences.

27. Although the data breach has occurred, Equifax continues to maintain the PII of consumers, including Plaintiffs and members of the Class. Because Equifax has demonstrated an incapability to prevent another data breach, to mitigate damages after detecting a breach, and to timely warn consumers their PII has been compromised, Plaintiffs and members of the Class have an overriding interest to ensure their PII has been secured and will be secure in the future.

IV. FACTS SPECIFIC TO NAMED PLAINTIFFS

a. Plaintiff Sabina Bologna

28. Plaintiff Sabina Bologna has been a direct customer of Equifax.

29. On or about September 6, 2017, Ms. Bologna received an email from Best Buy regarding a purchase of an iPad that she did not make herself. Concerned, Ms. Bologna logged onto Best Buy's website and saw that an iPad had been purchased using a Visa card in her name. It became apparent

to Ms. Bologna that she had been the victim of identity theft as an unauthorized person had opened a Visa account under her name and had used the unauthorized Visa card to purchase an Ipad. Ms. Bologna contacted Visa to attempt to resolve the identity theft issue. Visa, however, has been unable to resolve the identity theft matter and, upon information and belief, the unauthorized credit card continues to be used by an unauthorized person and Ms. Bologna's identity theft has not been resolved.

30. In response to the foregoing, in addition to contacting Visa, Ms. Bologna filed a police report, a fraud alert with all three major credit bureaus, and a report with the Federal Trade Commission.

b. Plaintiff Lucia Larocchia

31. Plaintiff Lucia Larocchia has been a direct customer of Equifax for years.

32. On or about July 31, 2017, Ms. Larocchia received a call from Sears. Sears notified Ms. Larocchia that someone was actively trying to change information related to her Sears credit card and Sears asked her to confirm whether the request was from her. Ms. Larocchia advised Sears that she had not attempted to change any information related to her Sears card. Sears further inquired whether, on or about July 31, 2017, Ms. Larocchia had made two purchases on her card, for $577.22 and $684, respectively.

Ms. Larocchia advised Sears that she had not made such purchases. Based upon the information provided by Ms. Larocchia, Sears reversed the charges and sent Ms. Larocchia a letter with information about the events involving her Sears card.

33. In or around August 2017, the power at Ms. Larocchia's home spontaneously went out. Ms. Larocchia had paid her bills and she contacted the Nevada energy company to inquire as to why the power had gone out. The Nevada energy company told Ms. Larocchia that: a) she had asked the company to turn off the electricity at her home address; and b) she had advised the Nevada energy company that she had moved to a new address and that power should be turned on at the new address, an apartment. Ms. Larocchia informed the Nevada energy company she had given no such directions and had been timely paying her bills.

34. Concerned that she was the subject of identity theft, Ms. Larocchia engaged in regular contact with a representative of the Nevada energy company about the matter, and asked the representative to listen to recordings about changes that had been requested to be made to her account. The Nevada energy company listened to the recordings about the requested changes, and told her that, based upon its investigation, the person who had requested the changes had a voice that differed from Ms.

Larocchia, but had provided the Nevada energy company with Ms. Larocchia's social security number. Based upon its investigation, the Nevada energy company determined that Ms. Larocchia had been defrauded and advised her that if she paid them $176.37, they would restore power to her home; Ms. Larocchia made the payment and the Nevada energy company restored power to her home.

35. Ms. Larocchia learned from the Nevada energy company the name and address of the persons who had stolen her identity and requested the changes to her account(s). Ms. Larocchia went to the police about her stolen identity and is currently working with them regarding the matter.

36. Subsequently, in August 2017, Ms. Larocchia received a phone call from Citibank that informed her that someone was seeking to apply for a credit card in her name and inquired whether it was her that was applying for the card. Ms. Larocchia advised Citibank she had not applied for a credit card.

37. Ms. Larocchia received a letter from Equifax on or about August 31, 2017 stating that it had placed a freeze on her credit and a fraud alert on her Equifax account; however, she had never requested a credit freeze or fraud alert.

38. Thereafter, on or about September 5, 2017, Ms. Larocchia received a letter from Chase which informed her that someone had applied for a credit card

in her name and inquired whether it was her that had applied for the card. Ms. Larocchia contacted Chase and advised it that she had not applied for a credit card.

c. Plaintiff Emily Knowles

39. Plaintiff Emily Knowles recently learned of the data breach through reports in the media.

40. In response, Ms. Knowles visited www.equifaxsecurity2017.com to ascertain whether she was affected by the data breach. Ms. Knowles entered the necessary information several times and received inconsistent results regarding whether she had been affected by the data breach.

41. After receiving inconsistent results from the Equifax site, Ms. Knowles became concerned that she was impacted by the data breach. As a result of her concern about being impacted by the data breach, Ms. Knowles froze her credit at Transunion, Experian and Equifax.

d. Plaintiff Kristen Galloway

42. Plaintiff Kristen Galloway recently learned of the data breach through reports in the media.

43. In response, Ms. Galloway visited www.equifaxsecurity2017.com to ascertain whether she was affected by the data breach.

44. After entering the necessary information, the site said that Ms. Galloway may have been affected by the data breach.

45. Recently, Ms. Galloway's credit score dropped from 817 to 793, but she has not yet learned of any identity theft.

V. CLASS ALLEGATIONS

44. Plaintiffs seek relief on behalf of themselves and all other members of the Class (the "National Class"). Pursuant to Fed. R. Civ. P. 23(a), (b)(2), (b)(3) and (c)(4), Plaintiffs seek certification of a class defined as follows:

> All persons in the United States whose personal or financial information was compromised as a result of the data breach first disclosed by Equifax on or about September 7, 2017.

45. In the alternative to the National Class, Plaintiffs seek certification of a "Multistate Class", composed of statewide classes of persons from states with similar laws as applied to the facts of this case, defined as

> All persons in ([STATE[S]) whose personal or financial information was compromised as a result of the data breach first disclosed by Equifax on or about September 7, 2017.

or, in the alternative, a Georgia Class defined as follows:

> All persons in Georgia whose personal or financial information was compromised as a result of the data breach first disclosed by Equifax on or about September 7, 2017.

46. The National Class, Multistate Class, and Georgia Class are collectively referred to herein as the "Class."

47. Excluded from the above class is Equifax, including any of its officers, executives, affiliates, parents, subsidiaries, and employees, all persons who timely elect to be excluded from the Class, governmental entities, attorneys for the Class, all jurors including alternates who sit on the case, and the judges to whom this case is assigned, including their immediate family and court staff.

48. Plaintiffs hereby reserve the right to amend or modify the class definition with greater specificity or division after having an opportunity to conduct discovery. The proposed class meets the criteria for certification under Fed. R. Civ. P. 23.

49. **Numerosity.** Consistent with Rule 23(a)(1), the members of the Class are so numerous that the joinder of all members is impracticable. Although, the exact number of Class members is unknown to Plaintiffs at this time, the proposed Class includes hundreds of thousands, and potentially millions, of individuals whose PII is maintained by Equifax. Class members may be ascertained through objective means. Class members may be notified of the pendency of this action by recognized, court-

approved dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

50. **Commonality.** This action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

i. Whether Equifax had a duty to protect PII;

ii. Whether Equifax knew or should have known of the susceptibility of their security systems to a data breach;

iii. Whether Equifax's security measures to protect their systems were reasonable considering the measures recommended by data security experts;

iv. Whether Equifax was reckless or negligent in failing to implement reasonable and adequate security procedures and practices;

v. Whether Equifax's failure to implement adequate data security measures allowed the breach to occur;

vi. Whether Equifax's conduct was the proximate cause of the data breach;

vii. Whether Plaintiffs and Class members were injured and suffered damages or other acceptable losses because of Equifax's failure to reasonably protect its POS systems and data network; and

viii. Whether Plaintiffs and Class members are entitled to relief.

51. **Typicality**. Consistent with Fed. R. Civ. P. 23(a)(3), Plaintiffs' claims are typical of the Class. Plaintiffs had their PII placed at risk by the data

breach. Plaintiffs' damages and injuries are nearly identical to other Class members and Plaintiffs seek relief consistent with that of the Class.

52. **Adequacy**. Plaintiffs are adequate representatives of the Class because each plaintiff meets the definition of the proposed class and all are committed to pursuing this matter against Equifax to obtain relief for themselves and the Class. Plaintiffs have no conflicts of interest with the Class. Plaintiffs' counsel is competent and experienced in litigating class actions. Plaintiffs intend to prosecute this case and will fairly and adequately protect the interests of the Class.

53. **Superiority**. A class action is superior to any other method of relief for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify the maintenance of individual actions.

54. All members of the proposed class are ascertainable. Equifax maintains information regarding the data breach, including the relevant time periods and the identities of all affected consumers.

VI. CAUSES OF ACTION

COUNT I—NEGLIGENCE

53. Plaintiffs incorporate by reference the preceding paragraphs as if fully set forth herein.

54. Upon collecting and storing the PII of Plaintiffs and Class members in its computer systems and on its networks, Equifax undertook and owed a duty to Plaintiffs and the Class to exercise reasonable, prudent care to secure and safeguard their PII. Equifax knew that the PII was private and confidential and therefore must be protected so as not to subject Plaintiffs and Class members to any unreasonable risk of harm. Plaintiffs and the Class are foreseeable victims of inadequate cybersecurity. Equifax owed duties to Plaintiffs and the Class, including but not limited to (i) the duty to use reasonable and adequate security procedures and systems consistent with industry standards; (ii) the duty to timely detect cybersecurity incidents; and (iii) the duty to timely disclose to potentially affected persons the happening of a cybersecurity incident.

55. Equifax breached its legal duties when it failed to maintain adequate technological safeguards and deviated from the standard of care with respect to the collection, maintenance, storage, and holding of PII.

COUNT II—NEGLIGENCE PER SE

56. Plaintiffs incorporate by reference the preceding paragraphs as if fully set forth herein.

57. Section 5 of the Federal Trade Commission Act (the "FTC Act") prohibits "unfair . . . practices in or affecting commerce," including the unfair act or practice by businesses, such as Equifax, of failing to use reasonable measures to protect PII.

58. Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and failing to meet applicable industry standards. Equifax's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach.

59. Equifax's violation of the FTC Act constitutes negligence per se.

60. Plaintiffs and the Class members are within the class of persons the FTC Act is intended to protect.

61. The harm resulting from the data breach is of the type the FTC Act is intended to prevent.

COUNT III-WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT

62. Plaintiffs incorporate by reference the preceding paragraphs as if fully set forth herein.

63. Plaintiffs and the Class are consumers entitled to the protections of the Fair Credit Reporting Act ("FCRA"), 15 U.S.C. § 1681.

64. Under 15 U.S.C. § 1681a(f), a "consumer reporting agency" is defined as "any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.…"

65. Equifax is a consumer reporting agency under the FCRA because, for monetary fees, it regularly engages in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

66. As a consumer reporting agency, 15 U.S.C. § 1681e(a) requires Equifax to "maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this titl".

67. Under 15 U.S.C. § 1681a(d)(1), a "consumer report" is defined as:

> …any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for -- (A) credit . . . to be used primarily for personal, family, or household purposes; . . . or (C) any other purpose authorized under section 1681b of this title.

The compromised data was a consumer report under the FCRA because it was a communication of information bearing on Class members' creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living used, or expected to be used or collected in whole or in part, for the purpose of serving as a factor in establishing the Class members' eligibility for credit.

68. As a consumer reporting agency, Equifax may only furnish a consumer report under the limited circumstances set forth in 15 U.S.C. § 1681b, "and no other." 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b permit credit reporting agencies to furnish consumer reports to unauthorized or unknown entities, or hackers such as those who accessed the Class members' PII. Equifax violated § 1681b by furnishing consumer reports to unauthorized or unknown entities or computer hackers, as detailed above.

69. Equifax furnished the Class members' consumer reports by disclosing their consumer reports to unauthorized entities and hackers, allowing unauthorized entities and hackers to access their consumer reports, knowingly and/or recklessly failing to secure the PII from unauthorized entries, and failing to take reasonable, prudent security measures to prevent unauthorized entries.

70. Equifax willfully and/or recklessly violated § 1681b and § 1681e(a) by providing impermissible access to consumer reports and by failing to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. The willful and reckless nature of Equifax's violations is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, Equifax touts itself as an industry leader in breach prevention; thus, Equifax knew of the importance of the measures that must be taken to prevent data breaches and willingly failed to take them.

71. Equifax also acted willfully and recklessly because it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. *See*, *e.g.*, 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary on The Fair Credit Reporting Act. 16 Part 600, Appendix to Part 600, Sec. 607 2E. Equifax obtained or had available these and other substantial written materials that apprised them of their duties under the FCRA.

72. Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiffs' and Class members' PII for no permissible purpose.

73. Plaintiffs and the Class members have been damaged by Equifax's willful and/or reckless failure to comply with the FCRA. Therefore, Plaintiffs and each of the Class members are entitled to recover actual damages under 15 U.S.C. § 1681n(a)(1)(A) and any other applicable statute.

74. Plaintiffs and the Class are also entitled to punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a)(2) & (3).

COUNT IV-
NEGLIGENT VIOLATION OF
THE FAIR CREDIT REPORTING ACT

75. Plaintiffs incorporate by reference the preceding paragraphs as if fully set forth herein.

76. Equifax was negligent in failing to maintain reasonable procedures to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA. Equifax's negligent failure to maintain reasonable procedures is supported by, among other things, former employees' admissions that Equifax's data security practices have deteriorated in recent years, and Equifax's numerous other data breaches in the past. Further, as an enterprise claiming to be an industry leader in data breach

prevention, Equifax knew of the importance of the measures that should be taken to prevent data breaches, yet failed to take them.

77. Equifax's negligent conduct allowed unauthorized intruders to obtain Plaintiffs and the Class members' PII and consumer reports for no permissible purpose under the FCRA.

78. Plaintiffs and the Class members have been damaged by Equifax's negligent failure to comply with the FCRA. Therefore, Plaintiffs and each of the Class members are entitled to recover "any actual damages sustained by the consumer." 15 U.S.C. § 1681o(a)(1).

79. Plaintiffs and the Class members are also entitled to recover both costs of the action and reasonable attorney fees. 15 U.S.C. § 1681o(a)(2).

80. Upon information and belief, Equifax improperly and inadequately safeguarded PII of Plaintiffs and Class members, deviating from standard industry rules, regulations, and practices at the time of the unauthorized access. Equifax's failure to take proper security measures to protect sensitive PII of Plaintiffs and Class members created conditions conducive to an intentional criminal act.

COUNT V—DECLARATORY JUDGMENT

81. Plaintiffs incorporate by reference the preceding paragraphs as if fully set forth herein.

82. Plaintiffs and Class members entered into an implied contract with Equifax that required Equifax to provide adequate security for PII. As alleged herein, Equifax owes duties of care to Plaintiffs and Class members that require it to adequately secure PII.

83. Equifax still possesses and controls PII of Plaintiffs and Class members.

84. Equifax has not remedied the vulnerabilities of its cybersecurity system that lead to the data breach.

85. Equifax has thus not discharged its legal and contractual duties owed to Plaintiffs and the Class. In fact, since the data breach has now been made public, the PII in Equifax's possession is now more vulnerable than it was previously.

86. Actual harm has arisen in the wake of the data breach with respect to Equifax's obligations and duties of care to provide data security measures to Plaintiffs and the Class.

87. Therefore, Plaintiffs and the Class seek the Court to declare that: (a) Equifax's existing data security measures do not comply with its contractual obligations and duties of care, and (b) to comply with its contractual obligations and duties of care, Equifax must implement and maintain reasonable security measures, including but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated

attacks, penetration tests, and audits on Equifax's systems on a periodic basis, and ordering Equifax to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Segmenting PII by, among other things, creating firewalls and access controls so that if one area of Equifax is compromised, hackers cannot gain access to other portions of Equifax systems;

e. Purging, deleting, and destroying in a reasonable secure manner PII not necessary for its provisions of services;

f. Conducting regular database scanning and securing checks;

g. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Equifax customers must take to protect themselves

COUNT VI—UNJUST ENRICHMENT

88. Plaintiffs incorporate by reference all preceding paragraphs as if fully set forth herein.

89. Plaintiffs and the Class conferred a monetary benefit on Equifax. Specifically, Equifax profited from and used the PII of Plaintiffs and the

Class for business purposes. Equifax knew that Plaintiffs and the Class conferred a benefit on Equifax.

90. Equifax retained the benefit of not incurring the cost of adequate and proper data security measures at the expense of Plaintiffs and the Class.

91. Equifax acquired the PII through inequitable means as it failed to disclose the inadequate security practices alleged herein.

92. Under the circumstances, it would be unjust for Equifax to be permitted to retain any of the benefits conferred on it by Plaintiffs and the Class and that Equifax received at the expense of Plaintiffs and the Class.

COUNT VII
VIOLATION OF GEORGIA FAIR BUSINESS PRACTICES ACT
O.C.G.A. § 10-1-390, *et seq.*

93. Plaintiffs incorporate by reference all preceding paragraphs as though fully set forth herein.

94. The Georgia Fair Business Practice Act (FBPA), specifically O.C.G.A. § 10-31-393(a) forbids and declares unlawful any unfair or deceptive acts or practices in the conduct of consumer transactions and consumer acts or practices in trade or commerce. *Ussery v. Goodrich Restoration, Inc.*, 2017 WL 2119163 (Ga. App. May 16, 2017). A single instance of an unfair or deceptive trade act or practice is a sufficient predicate upon which to base

a claim for damages under the Fair Business Practices Act (FBPA) if the public consumer interest would be served thereby. *Isbell v. Credit Nation Lending Service, LLC*, 735 S.E.2d 46 (Ga. App. 2012).

95. Equifax violated the FBPA when it engaged in unfair and deceptive acts and practices in connection with the data breach, including:

a. the failure to adequately protect, secure, and safeguard PII despite being a major United States credit bureau and knowing the likely result of a data breach;

b. the failure to warn consumers before the data breach that their PII was inadequately safeguarded;

c. the failure to both timely and adequately disclose the data breach to the Plaintiffs and the Class

d. Continuing to operate in the ordinary course of business with consumers' PII immediately after discovering the data breach

e. Purposefully delaying public disclosure of the data breach for approximately six weeks, despite understanding and knowing the gravity of the event

f. Allowing its senior executives to trade shares of stock and exercise options immediately after discovering the data breach and in anticipation of a dramatic decrease in the value of Equifax shares

96. Equifax either knew or should have known its cybersecurity system was inadequate to safeguard PII, that a data breach was likely to occur, and that Equifax would not be able to timely detect a data breach should one happen.

97. As a direct and proximate consequence of Equifax's violation, Plaintiffs and the Class are entitled to damages and equitable relief, as set forth herein.

98. Plaintiffs bring this action on behalf of themselves and the putative class. This action promotes the public interest and the public will benefit from this action, including protecting the public from Equifax's unfair, deceptive, and unlawful practices.

99. Pursuant to the FBPA, Plaintiffs and the Class are entitled to damages, including all actual and consequential damages, punitive damages, costs, attorney's fees, and all such other further relief as the Court may deem proper and allowable by law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Equifax as follows:

a. For an Order certifying the Class, as defined herein, and appointing Plaintiffs and their counsel to represent the Class;

b. For equitable relief enjoining Equifax from engaging in the wrongful conduct complained of herein and pertaining to the misuse and/or disclosure of Plaintiffs' and the Class members' PII, and from refusing to issue timely, complete and accurate disclosures to the Plaintiffs and the Class;

c. For equitable relief, compelling Equifax to use appropriate cyber security methods and policies with respect to consumer data collection, storage, and protection, and to disclose with specificity to Class members the type of PII compromised;

d. For an award of damages, as allowed by law and in an amount to be determined by a jury;

e. For an award of attorneys' fees, costs, and litigation expenses, as allowable by law;

f. For prejudgment interest on all amounts awarded; and

g. Such other and further relief as this court may deem just and proper.

Pursuant to Fed. R. Civ. P. 38(b), Plaintiffs demand a trial by jury.

Respectfully submitted: September 15, 2017

/s/ Jonathan W. Johnson
Jonathan W. Johnson
Georgia Bar No. 394830
Jonathan W. Johnson, LLC
2296 Henderson Mill Rd., Suite 304
Atlanta, GA 30345
Phone: 404-298-0795
Fax: 404941-2285
Email: jwj@johnson-lawyer.com

/s/ Mark J. Geragos

Mark Geragos (pending admission *pro hac vice*)
Ben Meiselas (pending admission *pro hac vice*)
Lori G. Feldman (pending admission *pro hac vice*)
GERAGOS & GERAGOS
Historic Engine Co. No. 28
644 South Figueroa St.
Los Angeles, California 90017
geragos@geragos.com
Phone 213-625-3900